BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Pada penelitian ini Algoritma Enkrispsi RSA1024 telah berhasil diimplementasikan pada pengiriman kunci Salsa20 dan Algoritma Enkrispsi Salsa20 berhasil diimplementasikan. Algoritma Enkripsi Salsa20 memiliki hasil yang sama pada aplikasi yang menggunakan *library* dengan aplikasi tanpa *library*. Pada Algoritma Enkripsi RSA 1024 memiliki hasil yang sama pada aplikasi dan Mobilefish.

Pada uji coba ARP *spoofing*, uji coba dilakukan dengan sesama pengguna dengan melakukan panggilan dan dilakukan penyadapan. Hasil pengujian menunjukkan bahwa penyadap hanya mendapatkan suara yang tidak jelas dan pecah, serta kunci Salsa20 sepanjang 172 karakter yang seharusnya 16 karakter, dan IV Salsa20 sepanjang 172 karakter yang seharusnya 8 karakter.

Dalam menghitung *processing delay*, waktu proses awal inisialisasi panggilan, aplikasi yang menggunakan enkripsi memiliki waktu proses sebesar 3 menit 50,186 detik pada sisi pengirim, dan 14,301 detik pada sisi penerima, sehingga waktu proses awal inisialisasi panggilan memiliki *processing delay* yang tidak dapat ditoleransi. Tetapi nilai *processing delay* saat melakukan panggilan, memiliki nilai 23,07 ms pada sisi pengirim, dan 21,416 ms pada sisi penerima, sehingga *processing delay* masih dapat diterima.

Pada uji coba jitter, rata – rata *jitter* pada aplikasi yang tidak menggunakan enkripsi adalah 10 ms dan *jitter* maksimum adalah 10,95 ms. Pada aplikasi yang menggunakan enkripsi rata – rata *jitter* adalah 10 ms dan *jitter* maksimal adalah

10,44 ms. Dengan kata lain aplikasi yang menggunakan enkripsi memiliki *jitter* yang lebih kecil dibandingkan aplikasi yang tidak menggunakan enkripsi. Pada *throughput* keduanya memiliki selisih rata – rata *throughput* yaitu 75,73 B/sec dimana aplikasi yang menggunakan enkripsi memiliki *throughput* lebih kecil yaitu 16.422,82 B/sec.

5.2 Saran

Pada penelitian berjudul "Implementasi Algoritma RSA 1024 dan Salsa20 Dalam Pengiriman Data Aplikasi Komunikasi Berbasis VoIP" memiliki saran dalam penelitian ini, yaitu sebagai berikut.

1. Menggunakan blok kunci sepanjang 2048 bit atau lebih untuk algoritma enkripsi RSA. Karena berdasarkan pada Hukum Moore, jumlah transistor pada *chip* meningkat dua kali lipat setiap tahun (Meindl, 2003). Yang berarti kekuatan kunci yang sekarang memadai akan segera usang.
2. Algoritma enkripsi Salsa20 dapat diimplementasikan untuk melakukan enkripsi data pada aplikasi yang memiliki fitur *video call*.
3. Menggunakan *library* RSA 1024 yang disediakan oleh Visual Studio dengan memasukkan DLL System.Security.Cryptography dan menggunakan kode pada program "using System.Security.Cryptography".